

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Dropbox account DROPBOXVIDS4@GMAIL.COM

Case No. 14- 1274-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252	Illegal distribution, receipt, and possession of child pornography
18 U.S.C. 2251	Use of a minor to produce images of a child engaged in sexually explicit conduct

The application is based on these facts:
See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

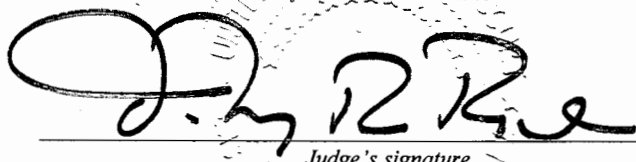
Jennifer Morrow, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/10/2014

City and state: Philadelphia, Pennsylvania



Judge's signature

Honorable Timothy R. Rice

Printed name and title

14-1274

AFFIDAVIT

I, Jennifer A Morrow, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI for 12 years, and am currently assigned to the Philadelphia Division's Violent Crimes Against Children Squad in the Newtown Square Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to violent crime, drug trafficking, kidnapping, and the FBI's Innocent Images National Initiative, which investigates matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, training at the Innocent Images Unit of the FBI, various conferences involving Innocent Images and Crimes Against Children, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements in this Affidavit are based on my investigation and other law enforcement officers' investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2251, 2252(a)(2), and 2252(a)(4)(B) are located at:

- a. Google Inc. and associated with the account DROPBOXVIDS4@GMAIL.COM, listed in attachment A-1, for the items specified in Attachment B-1 hereto.

b. Dropbox Account DROPBOXVIDS4@GMAIL.COM, listed in Attachment A-2, for the items specified in Attachment B-2 hereto.

LEGAL AUTHORITY

4. Title 18 U.S.C. Section 2251(a) prohibits a person from using the mail or any facility, including the computer, or means of interstate or foreign commerce, from knowingly employing, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

5. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

6. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Google, Hotmail, Dropbox, and Apple. I request that the providers be required to produce the electronic communications and other information identified in Attachments A and B hereto. Because the service providers are not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring the service providers to perform the search would be a burden upon the company. If all they are asked to do is produce all the files associated with the account, an employee can do that easily. Requiring

them to search the materials to determine what content is relevant would add to their burden.

7. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Google, and Dropbox pursuant to the search warrant. In reviewing these files, I will treat them in the same way as if I were searching a file cabinet for certain documents. E-mails and chat logs will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

8. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

9. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing the service providers to comply even though they are not located in this district, because the Court has jurisdiction over the offense being investigated.

10. I also ask that the warrant direct the providers to produce records and other information pertaining to this account. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth below to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

11. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

12. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

13. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

14. Cell phones and more advanced devices known as "smart phones" function the same as computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.

15. I know from my experience and from talking with other agents that that iPhones can be backed up to a personal computer. When a person does this, by connecting the iPhone to the computer, a copy of the files contained on the iPhone is made and saved on the computer. In addition, more recent versions of the iPhone are encrypted. If the iPhone has been backed up to a computer, the computer will contain a file that will enable a forensic examiner to recover many files from the iPhone in spite of the encryption.

16. E-mail is a popular form of transmitting messages and or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

17. Internet-based e-mail is a service provided by an electronic communication service provider allowing individuals to send and receive e-mail from any Internet connected computer, regardless of their location or Internet service provider (ISP). Individuals utilizing Internet-based e-mail services access their accounts by "logging in" through the web-browser software installed on their computer, often by providing an account name and an associated password. Once the service provider's computers have determined the password is correct for the given account name, the individual "logged-in" can access any e-mail sent to their account, and or send e-mail to any other e-mail address accessible via the Internet.

18. Internet-based e-mail service providers reserve and or maintain computer disk storage space on their computer system, usually limited and closely regulated, for the use of the

service subscriber for the storage of e-mail communications with other parties, which include graphic files, programs, or other types of data stored in electronic form.

19. Internet-based e-mail service providers maintain records pertaining to the individuals who subscribe to their services. These records could include the account holder's name, address, date of birth, gender, occupation, and the Internet Protocol (IP) address used to establish the account and subsequent accesses to that account.

20. Any e-mail that is sent to a Internet-based e-mail subscriber is stored in the subscriber's "mail box" on the electronic communications service provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely. Electronic communications service provider's can also perform backups of subscriber's email accounts as routine maintenance in case their servers become inoperable so the content in the subscriber's account is not lost.

21. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. Most Internet-based e-mail users have the option of saving a copy of a sent e-mail. Unless the sender of the e-mail specifically deletes the e-mail from the provider's server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained by the provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

22. Internet-based e-mail provider's typically offer services to their subscribers that allow them to store any electronic file (i.e. image files, text files, etc.) on servers maintained and or owned by the provider.

23. E-mails and other electronic files stored on an electronic communications service provider's server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the provider's server.

24. G-mail is an Internet-based electronic communications system operated by Google. It permits its users to communicate using e-mail and other social networking type methods.

25. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at <https://www.dropbox.com/provacy>, Dropbox collects and stores "the files you upload, download, or access with the Dropbox service," and also collects logs: "When you use the Service, we automatically record information for your Device, its software, and your activity using he Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your files, and other interactions with the

Service., “Dropbox is a free service that let you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website.”

26. Dropbox client supports synchronization and sharing along with personal storage. It supports revision history, so files deleted from the Dropbox folder may be recovered from any of the synced computers. Dropbox supports multi-user version control, enabling several users to edit and re-post files without overwriting versions. Dropbox uses a freemium business model, where users are offered a free account with a set storage size and paid subscriptions for accounts with more capacity.

BACKGROUND OF THE INVESTIGATION

27. On or about May 27, 2014, an FBI Task Force Officer and Detective with the Metropolitan Police Department in Washington D.C. was online undercover and received an email from a Craigslist email account rst8v-4469957022@pers.craigslist.org in response to an advertisement placed by the undercover. In the email, rst8v-4469957022@pers.craigslist.org described himself as a bisexual male, 31 years of age, with a 2 year old daughter, and stated that he liked “licking my daughter, love super young.” During the email conversation rst8v-4469957022@pers.craigslist.org stated “just can’t help licking mine, it’s so irresistible...they taste so yummy at that age. Would love to jerk off with you sometime....and talk about it or share pics.” Based on your affiant’s training and experience, “licking my daughter” and “just can’t help licking mine” refer to oral sex, and “share pics” refers to his sharing child pornography.

28. The undercover stated he was on Yahoo! Instant Messenger and provided his user id to rst8v-4469957022@pers.craigslist.org, who told the undercover that he would add him to his list of contacts that night so that they could chat. All of the emails sent to the undercover from rst8v-4469957022@pers.craigslist.org stated at the bottom that they were "Sent from my iPhone."

29. During the Yahoo! chat session "got2hirejose" sent the undercover officer three images, all depicting child pornography, as described below:

a. Image titled "Image 02.jpg" is what appears to be a toddler wearing a pink top, possibly a bathing suit top, and nothing else. The toddler has her legs open displaying the vaginal area. The toddler has colored nail polish on her nails. The picture does not show the toddlers face but darker colored hair is visible.

b. Image titled "Image.jpg" is what appears to be an adult holding the four fingers of a prepubescent child. The adult is wearing what appears to be a silver ring on the ring finger of the left hand. The prepubescent child has colored nail polish on the nails and is wearing a shirt with a green colored sleeve. Upon review, your affiant believes the nail polish in this photograph is the same as the previous photograph. Your affiant believes that the adult holding up four fingers on the child is in response to the conversation between got2hirejose and the undercover outlined in the previous paragraph, in which the undercover requested evidence that got2hirejose was photographing a real child.

c. Image titled "Image 52714.jpg" is what appears to be a prepubescent child holding the penis of an adult male. The prepubescent child has colored nail polish on the nails and is wearing a shirt with a green colored sleeve. Upon review, your affiant

believes the prepubescent child in this photograph is the same as the previous photograph and the nail polish is the same as the previous photographs.

30. On May 28, 2014 an administrative subpoena was provided to Yahoo! Inc for subscriber and access log information associated with account "got2hirejose". Yahoo! subscriber listed Jose Gonzalez, Merchantville, NJ, 08109, and alternate email account GOT2HIREJOSE@GMAIL.COM. The account had been created on 10/28/2005. IP address 68.80.36.195 had been used to access the account on 05/27/2014 at 20:22 PT, 19:41 PT, and 19:18 PT, the times that the images were sent to the undercover officer.

31. On May 28, 2014, in response to an administrative subpoena served to Craigslist.org, the post identification of rst8v-4469957022@pers.craigslist.org was used by an individual using the email address GOT2HIREJOSE@GMAIL.COM.

32. Public database records show that IP address 68.80.36.195 was assigned by the Internet Service Provider (ISP) Comcast Communications. An emergency request to Comcast Communications for subscriber information associated with IP address 68.80.36.195 on 05/27/2014 at 20:22 PT, 19:41 PT, and 19:18 PT showed the subscriber to be Dennis Rzaca, telephone number 610-500-0768, VOIP number 484-840-8193, and service address of 4 Acorn Way, Glen Mills, PA 19342, the subject residence.

33. On May 28, 2014 a federal search warrant and arrest warrant were issued by the Eastern District of Pennsylvania for the search of 4 Acorn Way, Glen Mills, PA and the arrest of Jose Gonzalez.

34. Jose Gonzalez was arrested on May 29, 2014 and after waiving his Miranda rights gave a recorded statement to your affiant. In that statement Gonzalez admitted to taking pictures

of his 2 year old daughter and sending them to an individual that he originally met thru a craigslist advertisement. Gonzalez confirmed that the chats with this individual switched from craigslist to yahoo messenger. He stated that he knew it was wrong to send these pictures and that he sent them knowing that the other person was going to be sexually gratified by the images of his daughter. He repeatedly stated that he is "just a pervert." Gonzalez admitted that while chatting about sexually molesting his daughter, he was masturbating during the chat. He denied any intent to meet with the individual to trade his daughter for sex, as was discussed in the chat. Gonzalez offered that the other individual was more crude then him and that he is just easily influenced. He stated that last night was the first time he had touched his daughter inappropriately, but not the first time he had taken sexually explicit photographs of her.

35. Gonzalez identified his iPhone as the device that was used to take the pictures of his daughter, to chat with the other individual online, and to send the pictures of his daughter to that individual. He stated that he would take the pictures of his daughter, send them, and then delete them from the iPhone. Gonzalez identified his iPhone as the only iPhone in his vehicle at the time of his arrest.

36. During his communications with the undercover officer, Gonzalez stated that he stored all of his pictures and videos in his Dropbox account, which he identified as GOT2HIREJOSE2@ICLOUD.COM. GONZALEZ did not identify any other Dropbox accounts belonging to or utilized by him.

37. On 07/09/2104, a federal search warrant was issued to Dropbox for the account GOT2HIREJOSE2@ICLOUD.COM, the account identified by the subject during a Mirandized confession. A review of the results from that search warrant revealed approximately 50 photos of

child pornography and one video of child pornography. None of these included the photos of the victim that were taken by Gonzalez. Indeed, the photos of the victim were not recovered from any of Gonzalez' accounts, despite the defendant's confession that he took the photos of his daughter and distributed them to the undercover. In addition, Gonzalez admitted to possessing a large number of child pornography videos in his Dropbox account. As noted above, only one child pornography video was recovered from the Dropbox account that he identified for agents.

38. On 07/09/2014 a federal search warrant was issued on Google for the g-mail account identified by the target as belonging to him, specifically, GOT2HIREJOSE@GMAIL.COM. The results of the search warrant revealed an email to GONZALEZ from Gmail which discussed the opening of a new email account DROPBOXVIDS4@GMAIL.COM on 5/26/14, just one day before GONZALEZ began chatting with the undercover officer in this investigation. GONZALEZ failed to disclose this account to agents during his interview, even though specifically asked whether he had any additional accounts.

39. On 12/08/2014 an administrative subpoena was sent to DropBox regarding any subscriber information for the newly identified account of DROPBOXVIDS4@GMAIL.COM. Results are pending.

CONCLUSION


40. Based on the aforementioned factual information that the Craigslist.org ad was replied to by GOT2HIREJOSE@GMAIL.COM, with a transition to Yahoo messenger 'got2hirejose' which is subscribed to by GOT2HIREJOSE@HOTMAIL.COM, these accounts were used to communicate with an undercover officer and those communications were of a

sexual nature, your affiant respectfully submits that there is probable cause to believe that JOSE GONZALEZ has used the Google account GOT2HIREJOSE@GMAIL.COM to knowingly receive/distribute and or possess child pornography. In addition GONZALEZ used the remote storage accounts associated with Dropbox account GOT2HIREJOSE2@ICLOUD.COM to receive/distribute and/or possess child pornography. In addition GONZALEZ used that identified email account to establish two new accounts one day prior to his contact with the undercover officer online. These two new accounts were identified subsequent to a federal search warrant as DROPBOXVIDS4@GMAIL.COM. The affiant respectfully submits that there is probable cause to believe that GONZALEZ has violated Title 18, United States Code, Sections 2251, 2252(a)(2), and 2252(a)(4)(B). Additionally, there is probable cause to believe that evidence of the commission of these criminal offenses is associated with the following accounts:

- a. Google account DROPBOXVIDS4@GMAIL.COM and other computer servers of Google located at Google, 1600 Amphitheater Parkway, Mountain View, California,
- b. Dropbox Account DROPBOXVIDS4@GMAIL.COM and other computer servers of Dropbox located at 185 Berry Street, San Francisco, California

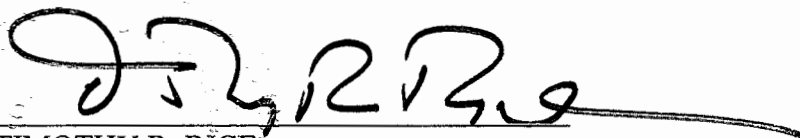
and this evidence, listed in Attachments A and B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

41. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachments A and B.



Jennifer A Morrow
Special Agent, Federal Bureau of Investigation

Sworn and subscribed
before me this 10 day of December, 2014.



TIMOTHY R. RICE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2

Location to be searched:

Dropbox account DROPBOXVIDS4@GMAIL.COM, which is stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, California 94107.

ATTACHMENT B-2

Items to be Seized associated with the account DROPBOXVIDS4@GMAIL.COM
(to be produced by Dropbox):

I. Information to be disclosed by Dropbox

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox including any messages, records, files, logs, or information that have been deleted but are still available to **Dropbox** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. DROPBOXVIDS4@GMAIL.COM
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized by the user;
- d. All records or other information stored by an individual using the account,
DROPBOXVIDS4@GMAIL.COM

e. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken.

(To be executed by Law Enforcement Agents)

Items to be seized:

- A. All files, documents, communications, images, videos, and contacts associated with the Dropbox account DROPBOXVIDS4@GMAIL.COM, related to child pornography, or to receive/distribute and/or possess child pornography, in violation of Title 18 U.S.C. Sections 2251, 2252(a)(2), and 2252(a)(4)(B) , along with any evidence that would tend to show the true identities of the persons committing these offenses.
- B. All available log files showing dates, times and IP addresses for access to these accounts.